RECEIVED
CENTRAL FAX CENTER

DEC 19 2006

Listing of Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application. This listing of the claims presumes that the amendments made in the Amendment mailed on December 4, 2006, have already been entered.

1. - 8. (Canceled).

9. - 16. (Canceled).

17. - 154. (Canceled).

155. (Currently amended) A method for verifying whether an e-mail sent by a sending party was accessed by an intended recipient, said method comprising:

a) storing recipient data pertaining to an actual recipient of e-mail in a data file, said stored data file containing identifying data that identifies said actual e-mail recipient and further being associated with said actual recipient's email address;

b) transmitting an e-mail from a sender computer to an intended recipient, the sender computer being connected to a communications network;

c) delivering said e-mail to an a recipient e-mail address;

d) detecting an access event, and discovering said stored data file that is associated with said actual recipient's e-mail address; and

e) sending identifying data contained in said discovered data file for confirming proper delivery of said e-mail.

156. Canceled.

157. (Previously presented) The method as in claim 155, wherein said access event comprises access of said e-mail that was delivered to said actual recipient e-mail address.

158. (Previously presented) The method as in claim 155, wherein said access event comprises access of an email account associated with said actual recipient e-mail address.

159. (Previously presented) The method as in claim 155, wherein said access event comprises activation of an e-mail processing software associated with said actual recipient e-mail address.

160. (Previously presented) The method as in claim 155, wherein the step of transmitting an e-mail from a sender computer includes attaching an executable attachment file in conjunction with the e-mail, the executable attachment file having a first module for discovering the stored data file that is associated with said actual recipient's email address and wherein the step of detecting an access event includes the step of executing the first module of the executable attachment file.

161. (Previously presented) The method as in claim 160, wherein the executable attachment file has a second module transmitted and delivered therewith, the second module for detecting the access event, and

further comprising the step of:

automatically executing the second module upon delivery of the attachment file to the actual recipient e-mail address.

162. Canceled.

163. (Currently amended) The method as in claim 155, wherein said actual recipient email address is associated with ~~an actual~~ a recipient computer.

164. (Currently amended) The method as in claim 163, wherein said ~~actual~~ recipient computer is a server of a service provider.

165. (Currently amended) The method as in claim 163, wherein said ~~actual~~ recipient computer is a user system that is directly accessible by the actual recipient, said user system including electronic mail processing software.

166. (Previously presented) The method as in claim 155, wherein a remote user computer may be used to gain remote access to said actual recipient e-mail address.

167. (Previously presented) The method as in claim 155, wherein said identifying data contained in said stored data file pertains to alphanumeric text identification, biometric identification, password identification, a computer generated user code, or a combination thereof.

168. (Previously presented) The method as in claim 155, wherein said stored data file comprises identity information that identifies an individual.

169. (Previously presented) The method as in claim 168, wherein said identity information pertains to biometric identification.

170. (Previously presented) The method as in claim 169 further comprising the step of recognizing biometric attributes of an individual.

171. **(Previously presented)** The method as in claim 168, wherein said identity information includes alphanumeric text identification information.

172. **(Previously presented)** The method as in claim 155, wherein said stored data file comprises information that identifies a business.

173. **(Previously presented)** The method as in claim 155, wherein said stored data file comprises information that identifies an organization.

174. **(Previously presented)** The method as in claim 155, wherein said stored data file comprises a computer generated user code.

175. **(Previously presented)** The method as in claim 155 further including the step of sending access event data of conditions attendant said access event.

176. **(Previously presented)** The method as in claim 155, wherein said actual recipient is an individual.

177. **(Previously presented)** The method as in claim 155, wherein said actual recipient is a business.

178. **(Previously presented)** The method as in claim 155, wherein said actual recipient is an organization.

179. (Previously presented) The method as in claim 155, wherein said step of sending identifying data is used to verify proper delivery of legal documents.

180. (Previously presented) The method as in claim 155, wherein said step of sending identifying data is used to verify proper delivery of confidential documents.

181. (Previously presented) The method as in claim 155, wherein said data file is stored on a computer associated with e-mail retrieval.

182. (Previously presented) The method as in claim 155, wherein said identifying data for confirming proper delivery of said e-mail is sent to an e-mail address.

183. Canceled.

184. (Currently amended) The method as recited in claim 258 wherein said step of sending recipient data for confirming proper delivery of said e-mail includes the steps of:

a) generating a confirmation of receipt notice wherein the inputted recipient data is included with said confirmation of receipt notice; and

b) sending said confirmation of receipt notice, wherein the inputted recipient data included with said confirmation of receipt notice can be compared to ~~delivery~~ information associated with said intended recipient in order to verify whether the ~~email~~ e-mail was accessed by the intended recipient.

185. (Previously presented) The method as in claim 236, wherein said access event comprises access of said e-mail that was delivered to said recipient e-mail address.

186. (Currently amended) The method as in claim 236, wherein said access event comprises access of an ~~email~~ e-mail account associated with said recipient e-mail address.

187. (Previously presented) The method as in claim 236, wherein said access event comprises activation of an e-mail processing software associated with said recipient e-mail address.

188. (Currently amended) The method as in claim 236, ~~further comprising the steps of:~~ wherein the step of transmitting an e-mail from a sender computer includes attaching ~~transmitting and delivering to the recipient e-mail address~~ an executable attachment file in conjunction with the e-mail, the executable attachment file having a first module for prompting the party who requested said access event to enter recipient data, ~~a second module for generating the confirmation of receipt notice, and a third module for transmitting the confirmation of receipt notice; and~~ ~~upon the detection of the access event, automatically executing the first, second, and third modules~~ and wherein the step of detecting an access event includes the step of executing the first module of the executable attachment file.

189. (Currently amended) The method as in claim 188, wherein the executable attachment file has a ~~fourth~~ second module transmitted and delivered therewith, the ~~fourth~~ second module for detecting the access event, and further comprising the step of automatically executing the ~~fourth~~ second module upon delivery of the attachment file to the recipient e-mail address.

190. Canceled.

191. (Previously presented) The method as in claim 236, wherein said recipient e-mail address is associated with a recipient computer.

192. (Previously presented) The method as in claim 191, wherein said recipient computer is a server of a service provider.

193. (Previously presented) The method as in claim 191, wherein said recipient computer is a user system that is directly accessible by a recipient, said user system including electronic mail processing software.

194. (Previously presented) The method as in claim 236, wherein said inputted recipient data pertains to alphanumeric text identification, biometric identification, password identification, a computer generated user code, or a combination thereof.

195. (Previously presented) The method as in claim 236, wherein said inputted recipient data comprises identity information that identifies an individual.

196. (Previously presented) The method as in claim 195, wherein said identity information pertains to biometric identification.

197. (Currently amended) The method as in claim 196 further comprising ~~means for~~ the step of recognizing biometric attributes of an individual.

198. (Previously presented) The method as in claim 195, wherein said identity information includes alphanumeric text identification information.

199. (Previously presented) The method as in claim 236, wherein said inputted recipient data comprises information that identifies a business.

200. (Previously presented) The method as in claim 236, wherein said inputted recipient data comprises information that identifies an organization.

201. (Previously presented) The method as in claim 236, wherein said inputted recipient data comprises a computer generated user code.

202. (Previously presented) The method as in claim 236 further including the step of sending access event data of attendant conditions of said access event.

203. (Previously presented) The method as in claim 236, wherein said recipient is an individual.

204. (Previously presented) The method as in claim 236, wherein said recipient is a business.

205. (Previously presented) The method as in claim 236, wherein said recipient is an organization.

206. (Previously presented) The method as in claim 236, wherein said inputted recipient data is used to verify proper delivery of legal documents.

207. (Previously presented) The method as in claim 236, wherein said inputted recipient data is used to verify proper delivery of confidential documents.

208. (Currently amended) The method recited by claim 260 wherein said step of sending recipient data for confirming proper delivery of said e-mail includes the steps of:

a) generating a confirmation of receipt notice wherein the acquired recipient data is included with said confirmation of receipt notice; and

b) sending said confirmation of receipt notice, wherein the acquired recipient data contained with said confirmation of receipt notice can be compared to ~~delivery~~ information associated with said intended recipient in order to verify whether the email was accessed by the intended recipient.

209. (Previously presented) The method as in claim 260, wherein said access event comprises access of said e-mail that was delivered to said recipient e-mail address.

210. (Currently amended) The method as in claim 260, wherein said access event comprises access of an ~~email~~ e-mail account associated with said recipient e-mail address.

211. (Previously presented) The method as in claim 260, wherein said access event comprises activation of e-mail processing software associated with said recipient e-mail address.

212. (Currently amended) The method as in claim 260, ~~further comprising the step of:~~ wherein the step of transmitting an e-mail from a sender computer includes attaching ~~transmitting and delivering to the recipient e-mail address~~ an executable attachment file in conjunction with the e-mail ~~file~~, the executable attachment file having a first module for acquiring recipient data that is related to biometric identification of the recipient, ~~a second module for generating the confirmation of receipt notice, and a third module for transmitting the confirmation of receipt notice;~~ and

~~upon the detection of the access event, automatically~~ wherein the step of detecting an access event includes the step of executing ~~at least~~ the ~~second and third modules~~ first module of the executable attachment file.

213. (Currently amended) The method as in claim 212, wherein the executable attachment file has a ~~fourth~~ second module transmitted and delivered therewith, the ~~fourth~~ second module for detecting the access event, and further comprising the step of:

automatically executing the ~~fourth~~ second module upon delivery of the attachment file to the recipient e-mail address.

214. Canceled.

215. (Previously presented) The method as in claim 260, wherein said recipient e-mail address is associated with a recipient computer.

216. (Previously presented) The method as in claim 215, wherein said recipient computer is a server of a service provider that is capable of receiving e-mail.

217. (Previously presented) The method as in claim 215, wherein said recipient computer is a user system that is directly accessible by the recipient, said user system including electronic mail processing software and being capable of receiving e-mail.

218. (Currently amended) The method as in claim 260, wherein said acquired recipient data is ~~further~~ related to a biometric imprint, alphanumeric text identification, password identification, a computer generated user code, or a combination thereof.

219. (Previously presented) The method as in claim 260, wherein said acquired recipient data comprises identity information that identifies an individual.

220. (Previously presented) The method as in claim 260 further comprising means for recognizing biometric attributes of an individual.

221. (Previously presented) The method as in claim 260, wherein said acquired recipient data comprises information that identifies a business.

222. (Previously presented) The method as in claim 260, wherein said acquired recipient data comprises information that identifies an organization.

223. (Previously presented) The method as in claim 260, wherein said acquired recipient data comprises a computer generated user code.

224. (Currently amended) The method as in claim 260 further including the step of ~~including in said confirmation of receipt notice~~ sending access event data of ~~attendant~~ conditions atendant ~~of~~ said access event.

225. (Previously presented) The method as in claim 260, wherein said recipient is an individual.

226. (Previously presented) The method as in claim 260, wherein said recipient is a business.

227. (Previously presented) The method as in claim 260, wherein said recipient is an organization.

228. (Currently amended) The method as in claim 260, wherein said ~~confirmation of receipt notice~~ sent recipient data is used to verify proper delivery of legal documents.

229. (Currently amended) The method as in claim 260, wherein said ~~confirmation of receipt notice~~ sent recipient data is used to verify proper delivery of confidential documents.

230. Canceled.

231. (Previously presented) The method as in claim 260, wherein said recipient data is acquired as a requisite condition for permitting access to said delivered e-mail.

232. (Previously presented) The method as in claim 260, wherein said recipient data is acquired as a requisite condition for permitting access to said recipient e-mail address.

233. (Previously presented) The method as in claim 260, wherein said recipient data is acquired as a requisite condition for operating a remote user computer, said remote user computer being operable to gain access to said recipient e-mail address.

234. (Previously presented) The method as in claim 260, wherein said recipient data is comprised of alphanumeric text, said alphanumeric text being associated with the at least one biometric attribute of said recipient.

235. (Previously presented) The method as recited in claim 256 wherein the step of sending at least some of the discovered identifying data for confirming proper delivery of said e-mail includes the steps of:

a) generating a confirmation of receipt notice wherein the acquired identifying data is included with said confirmation of receipt notice; and

b) sending said confirmation of receipt notice wherein the acquired identifying data contained with said confirmation of receipt notice can be compared to information associated with said intended recipient in order to verify whether the e-mail was accessed by the intended recipient.

236. (Previously presented) A method for verifying whether an e-mail sent by a sending party was accessed by an intended recipient, said method comprising:

a) transmitting an e-mail from a sender computer to an intended recipient, the sender computer being connected to a communications network;

b) delivering said e-mail to a recipient e-mail address;

c) detecting an access event, and prompting the party associated with said access event to input recipient data prior to allowing the requested access, said recipient data including identifying data related to the party associated with said requested access; and

d) sending recipient data for confirming proper delivery of said e-mail.

237. (Currently amended) The method recited by claim 264 wherein the step of sending data that identifies said recipient for confirming proper delivery of said e-mail includes the steps of:

a) generating a confirmation of receipt notice wherein the ~~acquired recipient~~ data that identifies the recipient is included ~~in~~ with said confirmation of receipt notice; and

b) sending said confirmation of receipt notice, wherein the ~~acquired recipient~~ data that identifies the recipient that is included ~~contained in~~ with said confirmation of receipt notice can be compared to ~~delivery~~ information associated with said intended recipient in order to verify whether the email was accessed by the intended recipient.

238. (Previously presented) The method as in claim 264, wherein said data that identifies said recipient is related to a biometric imprint, alphanumeric text identification, password identification, a computer generated user code, or a combination thereof.

239. (Currently amended) The method as in claim 264, wherein the data that identifies said recipient is comprised of alphanumeric text, said alphanumeric text being associated with ~~the~~ at least one biometric attribute of said recipient.

240. (Previously presented) The method as in claim 264 further including the step of recognizing biometric attributes of an individual.

241. (Previously presented) The method as in claim 264, wherein said data that identifies said recipient comprises identity information that identifies an individual.

242. (Previously presented) The method as in claim 264, wherein said data that identifies said recipient comprises information that identifies a business.

243. (Previously presented) The method as in claim 264, wherein said data that identifies said recipient comprises information that identifies an organization.

244. (Previously presented) A system for verifying whether e-mail sent by a sending party was accessed by an intended recipient, said system comprising:

a) a sender computer connected to a communications network and from which an email is transmitted;

b) a recipient computer connected to said communications network, said recipient computer capable of receiving said transmitted e-mail and further having a data storage for storing said received e-mail;

c) a data file stored on a computer associated with e-mail retrieval , said stored data file associated with a particular recipient e-mail address and identifying a party associated with said particular e-mail address;

d) software capable of detecting an access event, wherein, upon detecting said access event, said software discovers the stored data file that is associated with the particular e-mail address to which said e-mail was delivered; and

e) means for sending the discovered data file for confirming proper delivery of said e-mail.

245. (Previously presented) The system as in claim 275, wherein said access event comprises access of a delivered e-mail.

246. (Previously presented) The system as in claim 275, wherein said access event comprises access of an e-mail account associated with the e-mail address to which said e-mail was delivered.

247. (Previously presented) The system as in claim 275, wherein said access event comprises activation of the e-mail processing software associated with the e-mail address to which said e-mail was delivered.

248. (Previously presented) A system for verifying whether e-mail sent by a sending party was accessed by an intended recipient, said system comprising:

a) a sender computer connected to a communications network and from which an e-mail is transmitted;

b) a recipient computer connected to said communications network, said recipient computer capable of receiving said transmitted e-mail and further having data storage means for storing said received e-mail;

c) software capable of detecting an access event, wherein, upon detecting said access event, said software prompts the party associated with said access event to input recipient data prior to allowing the requested access, said recipient data comprising identifying data related to the party associated with said requested access; and

d) means for sending recipient data for confirming proper delivery of said e-mail.

249. (Previously presented) The system as in claim 248, wherein said access event comprises access of a delivered e-mail.

250. (Previously presented) The system as in claim 248, wherein said access event comprises access of an e-mail account associated with the e-mail address to which said e-mail was delivered.

251. (Previously presented) The system as in claim 248, wherein said access event comprises activation of e-mail processing software associated with the e-mail address to which said e-mail was delivered.

252. (Previously presented) A system for verifying whether e-mail sent by a sending party was accessed by an intended recipient, said system comprising:

a) a sender computer connected to a communications network and from which an e-mail is transmitted;

b) a recipient computer connected to said communications network, said recipient computer being capable of receiving said transmitted e-mail and further having data storage means

for storing said received e-mail;

c) biometric identification means for recognizing biometric attributes of an individual;

d) software capable of detecting an access event and identifying an individual through utilization of inputted biometric attributes of said individual; and

e) means for sending data that identifies said individual for confirming proper delivery of said e-mail.

253. (Previously presented) The system as in claim 252, wherein said access event comprises access of a delivered e-mail.

254. (Previously presented) The system as in claim 252, wherein said access event comprises access of an e-mail account associated with the e-mail address to which said e-mail was delivered.

255. (Previously presented) The system as in claim 252, wherein said access event comprises activation of e-mail processing software associated with the e-mail address to which said e-mail was delivered.

256. (Previously presented) A method for verifying whether an e-mail sent by a sending party was accessed by an intended recipient, said method comprising:

a) storing recipient data in a data file, said data file containing identifying data that identifies a recipient of e-mail and being associated with said recipient's e-mail address;

b) transmitting an e-mail from a sender computer to an intended recipient, the sender computer being connected to a communications network;

c) delivering said e-mail to an e-mail address;

d) detecting an access event, and discovering the stored data file that is associated with the

e-mail address to which said e-mail was delivered; and

e) sending at least some of the identifying data contained in said discovered data file for confirming proper delivery of said e-mail.

257. (Previously presented) A method for verifying whether an e-mail sent by a sending party was accessed by an intended recipient, said method comprising:

a) storing recipient data in a data file, said data file containing identifying data that identifies a recipient of e-mail and being associated with said recipient's e-mail address;

b) transmitting an e-mail from a sender computer to an intended recipient, the sender computer being connected to a communications network;

c) delivering said e-mail to an e-mail address;

d) detecting an access event, and discovering the stored data file that is associated with the e-mail address to which said e-mail was delivered; and

e) sending the discovered data file for confirming proper delivery of said e-mail.

258. (Previously presented) A method for verifying whether an e-mail sent by a sending party was accessed by an intended recipient, said method comprising:

a) transmitting an e-mail from a sender computer to an intended recipient, the sender computer being connected to a communications network;

b) delivering said e-mail to an e-mail address;

c) detecting an access event, and prompting the party that requested said access to input recipient data prior to allowing the requested access, said recipient data including identifying data that is associated with the party that requested said access; and

d) sending recipient data for confirming proper delivery of said e-mail.

259. (Previously presented) The method recited by claim 236 wherein said step of sending

recipient data for confirming proper delivery of said e-mail includes the steps of:

a) generating a confirmation of receipt notice wherein the inputted recipient data is included with said confirmation of receipt notice; and

b) sending said confirmation of receipt notice, wherein the inputted recipient data included with said confirmation of receipt notice can be compared to information associated with said intended recipient in order to verify whether the e-mail was accessed by the intended recipient.

260. (Previously presented) A method for verifying whether e-mail sent by a sending party was accessed by an intended recipient, said method comprising:

a) transmitting an e-mail from a sender computer to an intended recipient, the sender computer being connected to a communications network;

b) delivering said e-mail to a recipient e-mail address;

c) detecting an access event;

d) acquiring recipient data that is related to biometric identification of the recipient; and

e) sending recipient data for confirming proper delivery of said e-mail.

261. (Previously presented) The method as recited in claim 260 wherein said recipient data is acquired prior to said access event.

262. (Previously presented) The method as recited in claim 260 wherein said recipient data is acquired after said access event.

263. (Previously presented) The method as recited in claim 260 wherein said recipient data is sent to an e-mail address.

264. (Previously presented) A method for verifying whether e-mail sent by a sending party was

accessed by an intended recipient, said method comprising:

a) transmitting an e-mail from a sender computer to an intended recipient, the sender computer being connected to a communications network;

b) delivering said e-mail to an e-mail address;

c) identifying a recipient utilizing biometric identification;

d) detecting an access event; and

e) sending data that identifies said recipient for confirming proper delivery of said e-mail.

265. (Previously presented) The method as recited in claim 264 wherein said recipient is identified prior to said access event.

266. (Previously presented) The method as recited in claim 264 wherein said recipient is identified after said access event.

267. (Previously presented) The method as recited in claim 264 wherein said data that identifies said recipient is sent to an e-mail address.

268. (Previously presented) A method for verifying whether e-mail sent by a sending party was accessed by an intended recipient, said method comprising:

a) transmitting an e-mail from a sender computer to an intended recipient, the sender computer being connected to a communications network;

b) delivering said e-mail to an e-mail address;

c) identifying a recipient in association with biometric identification;

d) detecting an access event; and

e) sending data that identifies said recipient for confirming proper delivery of said e-mail.

269. (Previously presented) The method as in claim 268 wherein said recipient is identified prior to said access event.

270. (Previously presented) The method as in claim 268 wherein said recipient is identified after said access event.

271. (Previously presented) The method as in claim 268 wherein said data that identifies said recipient is sent to an e-mail address.

272. (Currently amended) A method for verifying whether an e-mail sent by a sending party was accessed by an intended recipient, said method comprising:

a) storing recipient data on a storage element of a computer that is used by a recipient of e-mail to access e-mail, said recipient data including identifying data that is associated with a recipient of e-mail;

b) transmitting an e-mail from a sender computer to an intended recipient, the sender computer being connected to a communications network;

c) delivering said e-mail to ~~an~~ a recipient e-mail address;

d) detecting an access event and discovering at least part of said stored recipient data that is associated with said recipient;

e) sending at least part of said discovered recipient data for confirming proper delivery of said e-mail.

273. (Previously presented) The method recited in claim 272 wherein said recipient of e-mail is an actual recipient of said e-mail.

274. (Previously presented) The method recited in claim 244 wherein said recipient of e-mail is an actual recipient of said e-mail.

275. (Previously presented) A system for verifying whether e-mail sent by a sending party was accessed by an intended recipient, said system comprising:

a) a sender computer connected to a communications network and from which an e-mail is transmitted;

b) a recipient computer connected to said communications network, said recipient computer capable of receiving said transmitted e-mail and further having a data storage for storing said received e-mail;

c) a data file stored on a computer, said stored data file containing identifying data pertaining to a party and associated with said party's e-mail address;

d) software capable of detecting an access event, wherein, upon detecting said access event, said software discovers identifying data contained in said stored data file that is associated with the e-mail address to which said e-mail was delivered; and

e) means for sending identifying data for confirming proper delivery of said e-mail.

276. (Previously presented) The system as recited in claim 275 wherein said recipient of e-mail is an actual recipient of said e-mail.

277. (Previously presented) The system as recited in claim 275 wherein said identifying data for confirming proper delivery of said e-mail is sent to an e-mail address.

278. (Previously presented) A system for verifying whether e-mail sent by a sending party was accessed by an intended recipient, said system comprising:

a) a sender computer connected to a communications network and from which an e-mail is transmitted;

b) a recipient computer connected to said communications network, said recipient computer capable of receiving said transmitted e-mail and further having a data storage for storing said received e-mail;

c) recipient data stored on the data storage of a computer that is used by a recipient of e-mail to access e-mail, said recipient data including identifying data that is associated with a recipient of e-mail;

d) software capable of detecting an access event, wherein, upon detecting said access event, said software discovers at least part of said stored recipient data that is associated with said recipient; and

e) means for sending at least part of said discovered recipient data for confirming proper delivery of said e-mail.

279. Canceled.

280. (Previously presented) The system as recited in claim 278, wherein said recipient data is contained in a
data file, said data file being stored on said storage of said computer.

281. (Previously presented) The system as recited in claim 278, wherein recipient data pertaining to said recipient of e-mail is stored on said storage prior to said access event.

282. (Previously presented) The system as recited in claim 278, wherein said at least part of said discovered recipient data for confirming proper delivery of said e-mail is sent to an e-mail address.

283. (Previously presented) The system as recited in claim 278, wherein said access event comprises access of a delivered e-mail.

284. (Previously presented) The system as recited in claim 278, wherein said access event comprises access of an e-mail account associated with the e-mail address to which said e-mail was delivered.

285. (Previously presented) The system as recited in claim 278, wherein said access event comprises activation of an e-mail processing software associated with the e-mail address to which said e-mail was delivered.

286. (Previously presented) The method as recited in claim 257 wherein the step of sending the discovered data file for confirming proper delivery of said e-mail includes the steps of:

a) generating a confirmation of receipt notice wherein the discovered data file is included with said confirmation of receipt notice; and

b) sending said confirmation of receipt notice, wherein the identifying data in the discovered data file that is included with said confirmation of receipt notice can be compared to information associated with said intended recipient in order to verify whether the email was accessed by the intended recipient.

287. (Previously presented) The method as recited in claim 272 wherein the step of sending at least part of said discovered recipient data for confirming proper delivery of said e-mail includes the steps of:

a) generating a confirmation of receipt notice wherein the discovered recipient data is included with said confirmation of receipt notice; and

b) sending said confirmation of receipt notice, wherein the discovered recipient data included with said confirmation of receipt notice can be compared to information associated with said intended recipient in order to verify whether the email was accessed by the intended recipient.

288. (Previously presented) The method as in claim 287, wherein said confirmation of receipt notice is sent to an e-mail address.

289. (Previously presented) The method as in claim 272, wherein said access event comprises access of said e-mail that was delivered to said recipient e-mail address.

290. (Previously presented) The method as in claim 272, wherein said access event comprises access of an e-mail account associated with said recipient e-mail address.

291. (Previously presented) The method as in claim 272, wherein said access event comprises activation of an e-mail processing software associated with said recipient e-mail address.

292. (Previously presented) The method as in claim 272, wherein the step of transmitting an e-mail from a sender computer includes attaching an executable attachment file in conjunction with the e-mail file, the executable attachment file having a first module for discovering the stored recipient data that is associated with said recipient, and wherein the step of detecting an access event includes the step of executing the first module of the executable attachment.

293. (Previously presented) The method as in claim 292, wherein the executable attachment file has a second module transmitted and delivered therewith, the second module for detecting the access event, and further comprising the step of:

automatically executing the second module upon delivery of the attachment file to said

recipient e-mail address.

294. (Previously presented) The method as in claim 272, wherein said recipient e-mail address is associated with a recipient computer.

295. (Previously presented) The method as in claim 294, wherein said recipient computer is a server of a service provider.

296. (Previously presented) The method as in claim 294, wherein said recipient computer is a user system that is directly accessible by a recipient, said user system including electronic mail processing software.

297. (Previously presented) The method as in claim 272, wherein a remote user computer may be used to gain remote access to said recipient e-mail address.

298. (Previously presented) The method as in claim 272, wherein said computer on which said recipient data is stored is a recipient computer.

299. (Previously presented) The method as in claim 272, wherein said computer on which said recipient data is stored is a remote user computer.

300. (Previously presented) The method as in claim 272, wherein said recipient data is contained in a data file, said data file being stored on said storage element of said computer.

301. (Previously presented) The method as in claim 272, wherein said storage element comprises of a hard disk drive.

302. (Previously presented) The method as in claim 272, wherein said storage element comprises of a memory module.

303. (Previously presented) The method as in claim 272, wherein recipient data pertaining to said recipient of e-mail is stored on said storage element prior to said access event.

304. (Previously presented) The method as in claim 272, wherein said stored recipient data pertains to alphanumeric text identification, biometric identification, password identification, a computer generated user code, or a combination thereof.

305. (Currently amended) The method as in claim 272, wherein said stored recipient data comprises~~, at least,~~ identity information that identifies an individual.

306. (Previously presented) The method as in claim 305, wherein said identity information pertains to biometric identification.

307. (Currently amended) The method as in claim 306 further comprising ~~means for~~ the step of recognizing biometric attributes of an individual.

308. (Previously presented) The method as in claim 305, wherein said identity information includes alphanumeric text identification data .

309. (Currently amended) The method as in claim 272, wherein said stored recipient data includes~~, at least,~~ information that identifies a business.

310. (Currently amended) The method as in claim 272, wherein said stored data includes~~, at least,~~ information that identifies an organization.

311. (Currently amended) The method as in claim 272, wherein said stored recipient data includes~~, at least,~~ a computer generated user code.

312. (Previously presented) The method as in claim 272 further including the step of sending access event data of attendant conditions of said access event.

313. (Previously presented) The method as in claim 272, wherein said recipient is an individual.

314. (Previously presented) The method as in claim 272, wherein said recipient is a business.

315. (Previously presented) The method as in claim 272, wherein said recipient is an organization.

316. (Previously presented) The method as in claim 272, wherein said sent recipient data is used to verify proper delivery of legal documents.

317. (Previously presented) The method as in claim 272, wherein said sent recipient data is used to verify proper delivery of confidential documents.

318. (Previously presented) The method as in claim 272, wherein said at least part of the discovered recipient data for confirming proper delivery of said e-mail is sent to an e-mail address.

319. (Previously presented) The method as recited in claim 256, wherein said identifying data for confirming proper delivery of said e-mail is sent to an e-mail address.

320. (Previously presented) The method as recited in claim 256, wherein said data file is stored on a computer associated with e-mail retrieval.

321. (Previously presented) The method as in claim 235, wherein said confirmation of receipt notice is sent to an e-mail address.

322. (Previously presented) The method as in claim 256, wherein said identifying data contained in said stored data file pertains to alphanumeric text identification, biometric identification, password identification, a computer generated user code, or a combination thereof.

323. (Previously presented) The method as in claim 257, wherein said data file is sent to an e-mail address.

324. (Previously presented) The method as in claim 257, wherein said data file is stored on a computer associated with e-mail retrieval.

325. (Previously presented) The method as in claim 286, wherein said confirmation of receipt notice is sent to an e-mail address.

326. (Previously presented) The method as in claim 257, wherein said identifying data contained in said stored data file pertains to alphanumeric text identification, biometric identification, password identification, a computer generated user code, or a combination thereof.

327. (Previously presented) The method as in claim 236, wherein said recipient data for confirming proper delivery of said e-mail is sent to an e-mail address.

328. (Previously presented) The method as in claim 236, wherein a remote user computer may be used to gain remote access to said recipient e-mail address.

329. (Previously presented) The method as in claim 236 wherein the party that is associated with said access event is an individual.

330. (Previously presented) The method as in claim 236 wherein the party that is associated with said access event is a business.

331. (Previously presented) The method as in claim 236 wherein the party that is associated with said access event is an organization.

332. (Previously presented) The method as in claim 258 wherein said recipient data for confirming proper delivery of said e-mail is sent to an e-mail address.

333. (Previously presented) The method as in claim 184, wherein said confirmation of receipt notice is sent to an e-mail address.

334. (Previously presented) The method as in claim 258, wherein said inputted recipient data pertains to alphanumeric text identification, biometric identification, password identification, a computer generated user code, or a combination thereof.

335. (Previously presented) The method as in claim 208, wherein said confirmation of receipt

notice is sent to an e-mail address.

336. (Previously presented) The method as in claim 260, wherein a remote user computer may be used to gain remote access to said recipient e-mail address.

337. (Previously presented) The method as in claim 219, wherein said identity information includes alphanumeric text identification.

338. (Previously presented) The method as in claim 237, wherein said confirmation of receipt notice is sent to an e-mail address.

339. (Previously presented) The method as in claim 268 , wherein said data that identifies said recipient is related to a biometric imprint, alphanumeric text identification, password identification, a computer generated user code, or a combination thereof.

340. (Currently amended) The method as in claim 268 further comprising ~~means for~~ the step of recognizing biometric attributes of an individual.

341. (Previously presented) A method for verifying whether an e-mail sent by a sending party was accessed by an intended recipient, said method comprising:

a) storing recipient data on a storage element of a computer that is used to access e-mail, said recipient data including identifying data that is associated with a recipient of e-mail;

b) transmitting an e-mail from a sender computer to an intended recipient, the sender computer being connected to a communications network;

c) delivering said e-mail to an e-mail address;

d) detecting an access event and discovering at least part of said stored recipient data that is associated with said recipient;

e) sending at least part of said discovered recipient data for confirming proper delivery of said e-mail.

342. (Previously presented) The system as in claim 244, wherein said discovered data file for confirming proper delivery of said e-mail is sent to an e-mail address.

343. (Previously presented) The system as in claim 244, wherein said access event comprises access of a delivered e-mail.

344. (Previously presented) The system as in claim 244, wherein said access event comprises access of an e-mail account associated with the e-mail address to which said e-mail was delivered.

345. (Previously presented) The system as in claim 244, wherein said access event comprises activation of an e-mail processing software associated with the e-mail address to which said e-mail was delivered.

346. (Previously presented) The system as in claim 248, wherein said recipient data for confirming proper delivery of said e-mail is sent to an e-mail address.

347. (Previously presented) The system as in claim 252, wherein said individual is identified prior to said access event.

348. (Previously presented) The system as in claim 252, wherein said individual is identified

after said access event.

349. (Previously presented) The system as in claim 252, wherein said data that identifies said individual for confirming proper delivery of said e-mail is sent to an e-mail address.